UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

ALEKSEI OLEGOVICH VOLKOV, A/K/A ALEKSEY OLEGOVICH VOLKOV, A/K/A ALEKSEQ OLEGOVI3 VOLKOV,

Defendant.

Cause No. 1:23-cr-

1:23-cr-0119 JRS MG

INDICTMENT

The Grand Jury charges that:

General Allegations

At times material to the charges in this Indictment:

Background Regarding Ransomware and Initial Access Brokers

1. Ransomware is a type of malicious software that prevents a user from accessing his computer and/or data. The computer and/or data are held for ransom and not released until payment is made to the person(s) who installed the ransomware. Ransomware actors generally require that payment be made with cryptocurrency (e.g., Bitcoin), and sometimes threaten to "leak" (i.e., publish) the user's data if payment is not made by a certain deadline.

2. Initial Access Brokers ("IABs") are individuals who unlawfully obtain access to computer networks, in the form of login credentials, and then sell the access for the purpose of financial gain. IABs sometimes sell access to individuals engaged in ransomware.

3. ALEKSEI OLEGOVICH VOLKOV, A/K/A ALEKSEY OLEGOVICH VOLKOV, A/K/A ALEKSEQ OLEGOVI3 VOLKOV, the defendant herein, was an IAB. VOLKOV obtained and sold access to the computer networks of businesses located in the United States for Bitcoin. VOLKOV worked with, and sold login credentials to, groups engaged in ransomware, in exchange for either an initial flat fee or a percentage of the ransom paid by the victim. The ransomware groups used the login credentials provided by VOLKOV to gain access to protected computers in the United States without authorization, deploy ransomware, and extort payment from victims.

Background Regarding BUSINESS 1

4. BUSINESS 1 was a law firm with its headquarters in Orlando, Florida. It engaged in business activities that affected interstate and foreign commerce.

5. PERSON 1 was an employee of BUSINESS 1.

6. BUSINESS 1 issued computer network login credentials to PERSON 1 consisting of an email address and password. The email address contained PERSON 1's first and last name. No one other than PERSON 1 was permitted to use the credentials to access BUSINESS 1's computer network.

7. The BUSINESS 1 network login credentials for PERSON 1 were a means of account access that could be used to obtain money, goods, services, and other things of value. This could be accomplished by deploying ransomware. Additionally, the login credentials could be used to obtain personal identifiable information about clients and employees of BUSINESS 1 and information about BUSINESS 1's trade secrets.

VOLKOV's Sale of PERSON 1's Login Credentials

8. On or about July 26, 2023, VOLKOV, the defendant herein, told PERSON 2 via an online instant messaging platform that he would sell login credentials for a United States business' computer network to PERSON 2 for $1,000.

9. On or about July 27, 2023, VOLKOV sent a screenshot to PERSON 2 of his computer screen while purporting to be logged into BUSINESS 1's network.

10. The same day, PERSON 2 agreed to purchase the credentials from VOLKOV for $1,000. VOLKOV provided PERSON 2 with a digital wallet address where PERSON 2 could send payment via Bitcoin. PERSON 2 then caused a quantity of Bitcoin valued at $1,000 at the time of the transfer to be transferred to the digital wallet address provided by VOLKOV. The Bitcoin transfer was initiated from Indianapolis, Indiana.

11. Following the Bitcoin transfer, VOLKOV told PERSON 2 that people generally buy login credentials from him "for lockers" (i.e., for the purpose of deploying ransomware) and "to download data."

12. After receiving the Bitcoin, VOLKOV electronically transferred the BUSINESS 1 network login credentials for PERSON 1 to PERSON 2. VOLKOV made the transfer while located outside the United States.

13. PERSON 2 received VOLKOV's transfer of the login credentials while located in Indianapolis, Indiana.

COUNT 1
18 U.S.C. §§ 1028(a)(7) and (b)(1)(D)
Unlawful Transfer of a Means of Identification

14. Paragraphs 1 through 13 of this Indictment are incorporated herein.

15. On or about July 27, 2023, within the Southern District of Indiana and elsewhere, ALEKSEI OLEGOVICH VOLKOV, A/K/A ALEKSEY OLEGOVICH VOLKOV, A/K/A ALEKSEQ OLEGOVI3 VOLKOV, the defendant herein, did knowingly transfer, possess, and use, in and affecting interstate and foreign commerce, without lawful authority, a means of identification of another person, to wit, the BUSINESS 1 network login credentials for PERSON 1, knowing that the means of identification belonged to another actual person, with the intent to commit, aid and abet, and in connection with, unlawful activity that constitutes a violation of Federal law, to wit, Access Device Fraud, in violation of Title 18, United States Code, Section 1029(a)(2), Obtaining Information from a Protected Computer, in violation of Title 18, United States Code, Section 1030(a)(2)(C), and Trafficking in Access Information, in violation of Title 18, United States Code, Section 1030(a)(6)(A), and, as a result of the offense, between on or about August 1, 2022 and August 1, 2023, the defendant did obtain things of value aggregating $1,000, to wit, a quantity of Bitcoin valued at $1,000 at the time of the transfer.

All of which is in violation of Title 18, United States Code, Sections 1028(a)(7) and (b)(1)(D).

COUNT 2
18 U.S.C. §§ 1030(a)(6)(A) and (c)(2)(A)
Trafficking in Access Information

16. Paragraphs 1 through 13 of this Indictment are incorporated herein.

17. On or about July 27, 2023, within the Southern District of Indiana and elsewhere, ALEKSEI OLEGOVICH VOLKOV, A/K/A ALEKSEY OLEGOVICH VOLKOV, A/K/A ALEKSEQ OLEGOVI3 VOLKOV, the defendant herein, did knowingly and with intent to defraud traffic in a password and similar information through which a computer may be accessed without authorization by transferring the BUSINESS 1 network login credentials for PERSON 1 to PERSON 2, and such trafficking affected interstate and foreign commerce.

All of which is in violation of Title 18, United States Code, Sections 1030(a)(6)(A) and (c)(2)(A).

COUNT 3
18 U.S.C. §§ 1029(a)(2) and (c)(1)(a)(i)
Access Device Fraud

18. Paragraphs 1 through 13 of this Indictment are incorporated herein.

19. On or about July 27, 2023, within the Southern District of Indiana and elsewhere, ALEKSEI OLEGOVICH VOLKOV, A/K/A ALEKSEY OLEGOVICH VOLKOV, A/K/A ALEKSEQ OLEGOVI3 VOLKOV, the defendant herein, did knowingly and with intent to defraud traffic in and use an unauthorized access device by transferring the BUSINESS 1 network login credentials for PERSON 1 to PERSON 2, and by such conduct, between on or about August 1, 2022 and August 1, 2023, did obtain things of value aggregating $1,000, to wit, a quantity of Bitcoin valued at $1,000 at the time of the transfer, and said trafficking affected interstate and foreign commerce.

All of which is in violation of Title 18, United States Code, Sections 1029(a)(2) and (c)(1)(a)(i).

COUNT 4
18 U.S.C. §§ 1028A(a)(1) and (b)
Aggravated Identity Theft

20. Paragraphs 1 through 13 of this Indictment are incorporated herein.

21. On or about July 27, 2023, within the Southern District of Indiana and elsewhere, ALEKSEI OLEGOVICH VOLKOV, A/K/A ALEKSEY OLEGOVICH VOLKOV, A/K/A ALEKSEQ OLEGOVI3 VOLKOV, the defendant herein, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, to wit, the BUSINESS 1 network login credentials for PERSON 1, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, Access Device Fraud, as alleged in Count 3 of this Indictment, knowing that the means of identification belonged to another actual person.

All of which is in violation of Title 18, United States Code, Sections 1028A(a)(1) and (b).

FORFEITURE

1. The allegations contained in Count 1 of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1028(b)(5).

2. Upon conviction of the offense in violation of Title 18, United States Code, Section 1028 set forth in Count 1 of this Indictment, the defendant, ALEKSEI OLEGOVICH VOLKOV, A/K/A ALEKSEY OLEGOVICH VOLKOV, A/K/A ALEKSEQ OLEGOVI3 VOLKOV, shall forfeit to the United States of America:

a. pursuant to Title 18, United States Code, Section 982(a)(2)(B), any property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of such violation; and

b. pursuant to Title 18, United States Code, Section 1028(b)(5), any personal property used or intended to be used to commit the offense.

3. The allegations contained in Count 2 of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i).

4. Upon conviction of the offense in violation of Title 18, United States Code, Section 1030 set forth in Count 2 of this Indictment, the defendant, ALEKSEI OLEGOVICH VOLKOV, A/K/A ALEKSEY OLEGOVICH VOLKOV, A/K/A ALEKSEQ OLEGOVI3 VOLKOV, shall forfeit to the United States of America:

a. pursuant to Title 18, United States Code, Section 982(a)(2)(B), any property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of such violation; and

b. pursuant to Title 18, United States Code, Section 1029(c)(1)(C), any personal property used or intended to be used to commit the offenses.

5. The allegations contained in Count 3 of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1029(c)(1)(C).

6. Upon conviction of the offense in violation of Title 18, United States Code, Section 1029 set forth in Count 3 of this Indictment, the defendant, ALEKSEI OLEGOVICH

VOLKOV, A/K/A ALEKSEY OLEGOVICH VOLKOV, A/K/A ALEKSEQ OLEGOVI3 VOLKOV, shall forfeit to the United States of America:

a. pursuant to Title 18, United States Code, Section 982(a)(2)(B), any property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of such violation; and

b. pursuant to Title 18, United States Code, Section 1029(c)(1)(C), any personal property used or intended to be used to commit the offense.

7. As to all counts, the property to be forfeited includes, but is not limited to, a black ASUS X500L-XO037H laptop computer bearing serial number D9N0CV358934393, an Apple iPhone 13 Pro bearing IMEI number 353639680939640, a black and blue Transcend USB flash drive, all accessories and parts recovered with the laptop computer, phone, and flash drive, and a money judgment.

8. If any of the property subject to forfeiture, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code,

Sections 982(b)(1), 1028(g), 1029(c)(2), and 1030(i), and Title 28, United States Code, Section 2461(c).

A TRUE BILL:

[redacted]

ZACHARY A. MYERS
United States Attorney

By: [signature]
MaryAnn T. Mindrum
Matthew B. Miller
Assistant United States Attorneys
KMS